Final Interference Search & Search

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	3574	713/193 OR 380/28 OR 380/37 OR 380/268	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/31 09:33
L2	276	708/203	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/31 09:25
L3	3841	1 OR 2	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/31 09:25
L4	295	3 AND ENCRYPT$3 AND BLOCK$1 AND (IV OR "INITALIZATION VECTOR")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/31 09:27
L5	288	(HWA.INV. AND JOHN) OR (PAMARTHY.INV. AND LAKSHMANA)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/31 09:29
L6	285	(HILL.INV. AND RALPH) OR (SWENSON.INV. AND ERIC) OR (FUTAGAMI.INV. AND MOTOMASA) OR (MITUZAWA.INV. AND ATSUSHI)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/31 09:31
L7	11292	5 OR 6	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/31 09:31
L8	5	5 AND 6	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/31 09:31

PORTAL
USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

encrypt$3 and block$3 and iv

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used **encrypt$3** and **block$3** and **iv**

Found **168** of **166,357**

Sort results by: relevance

Display results: condensed form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 168

Result page: **1** 2 3 4 5 6 7 8 9 next

Relevance scale

1 Security Mechanisms in High-Level Network Protocols
Victor L. Voydock, Stephen T. Kent
June 1983 **ACM Computing Surveys (CSUR)**, Volume 15 Issue 2
Publisher: ACM Press
Full text available: pdf(3.23 MB) Additional Information: full citation, references, citings

2 Algorithm 529: Permutations To Block Triangular Form [F1]
I. S. Duff, J. K. Reid
June 1978 **ACM Transactions on Mathematical Software (TOMS)**, Volume 4 Issue 2
Publisher: ACM Press
Full text available: pdf(199.04 KB) Additional Information: full citation, references, citings, index terms

3 System architecture of parallel processing system -Harry-
H. Yamana, T. Marushima, T. Hagiwara, Y. Muraoka
June 1988 **Proceedings of the 2nd international conference on Supercomputing**
Publisher: ACM Press
Full text available: pdf(1.54 MB) Additional Information: full citation, abstract, references, citings, index terms

4 A graphical approach to coset enumeration
Lucien A. Dimino
July 1971 **ACM SIGSAM Bulletin**, Issue 19
Publisher: ACM Press
Full text available: pdf(2.05 MB) Additional Information: full citation, abstract, references

5 On the emulation of flowcharts by decision tables
Art Lew
December 1982 **Communications of the ACM**, Volume 25 Issue 12
Publisher: ACM Press
Full text available: pdf(1.13 MB) Additional Information: full citation, abstract, references, citings, index terms

6 An Efficient Algorithm for Graph Isomorphism
D. G. Corneil, C. C. Gotlieb
January 1970 **Journal of the ACM (JACM)**, Volume 17 Issue 1
Publisher: ACM Press

Full text available: pdf(767.75 KB) Additional Information: full citation, references, citings, index terms

7 Dynamic slot allocation (DSA) in indoor SDMA/TDMA using smart antenna basestation □
Faisal Shad, Terence D. Todd, Vytas Kezys, John Litva
February 2001 **IEEE/ACM Transactions on Networking (TON)**, Volume 9 Issue 1
Publisher: IEEE Press
Full text available: pdf(208.90 KB) Additional Information: full citation, references, citings, index terms

8 Manufacturing applications: Neutral information structure for manufacturing simulations: designing reusable simulation modules for electronics manufacturing systems □
Phani S. Mukkamala, Jeffrey S. Smith, Jorge F. Valenzuela
December 2003 **Proceedings of the 35th conference on Winter simulation: driving innovation**
Publisher: Winter Simulation Conference
Full text available: pdf(449.49 KB) Additional Information: full citation, abstract, references

9 Path delay fault testing of ICs with embedded intellectual property blocks □
D. Nikolos, Th. Haniotakis, H. T. Vergos, Y. Tsiatouhas
January 1999 **Proceedings of the conference on Design, automation and test in Europe**
Publisher: ACM Press
Full text available: pdf(54.95 KB) Additional Information: full citation, citings, index terms

10 Use of computers in treating nonnumerical mathematics and group theoretical problems in physics □
Stig Flodmark, Esko Blokker
July 1970 **ACM SIGSAM Bulletin**, Issue 15
Publisher: ACM Press
Full text available: pdf(1.22 MB) Additional Information: full citation, abstract, references

11 Simulation model to evaluate operational system performance and repair shop workloads at a navy field site □
James T. Newell
March 1981 **Proceedings of the 14th annual symposium on Simulation**
Publisher: IEEE Press
Full text available: pdf(1.20 MB) Additional Information: full citation, abstract, references, index terms

12 Efficient 3-D range searching in external memory □
Darren Erik Vengroff, Jeffrey Scott Vitter
July 1996 **Proceedings of the twenty-eighth annual ACM symposium on Theory of computing**
Publisher: ACM Press
Full text available: pdf(877.45 KB) Additional Information: full citation, references, citings, index terms

13 GPSS V model of a computerized manufacturing system □
James R. Siebauer
December 1979 **Proceedings of the 11th conference on Winter simulation - Volume 2**
Publisher: IEEE Press
Full text available: pdf(813.68 KB) Additional Information: full citation, abstract, references, citings, index terms

14 A language for describing the functions of synchronous systems □
David L. Parnas

February 1966 **Communications of the ACM**, Volume 9 Issue 2
Publisher: ACM Press
Full text available: pdf(695.47 KB) Additional Information: full citation, abstract, references, citings

15 Automatic generation of DAG parallelism □
R. Cytron, M. Hind, W. Hsieh
June 1989 **ACM SIGPLAN Notices , Proceedings of the ACM SIGPLAN 1989 Conference on Programming language design and implementation PLDI '89**, Volume 24 Issue 7
Publisher: ACM Press
Full text available: pdf(1.58 MB) Additional Information: full citation, references, citings, index terms

16 Computer Communication Networks: Approaches, Objectives, and Performance Considerations □
Stephen R. Kimbleton, G. Michael Schneider
September 1975 **ACM Computing Surveys (CSUR)**, Volume 7 Issue 3
Publisher: ACM Press
Full text available: pdf(3.99 MB) Additional Information: full citation, references, citings, index terms

17 On an automated method □
Paul E. Hamburger
January 1966 **Proceedings of the 1966 21st national conference**
Publisher: ACM Press
Full text available: pdf(825.37 KB) Additional Information: full citation, abstract, references, citings, index terms

18 Partial redundancy elimination in SSA form □
Robert Kennedy, Sun Chan, Shin-Ming Liu, Raymond Lo, Peng Tu, Fred Chow
May 1999 **ACM Transactions on Programming Languages and Systems (TOPLAS)**, Volume 21 Issue 3
Publisher: ACM Press
Full text available: pdf(704.71 KB) Additional Information: full citation, abstract, references, citings, index terms

19 False sharing problems in cluster-based disk arrays □
Hai Jin, Kai Hwang
February 1999 **Proceedings of the 1999 ACM symposium on Applied computing**
Publisher: ACM Press
Full text available: pdf(618.92 KB) Additional Information: full citation, references, index terms

20 Statistical estimators for aggregate relational algebra queries □
Wen-Chi Hou, Gultekin Ozsoyoglu
December 1991 **ACM Transactions on Database Systems (TODS)**, Volume 16 Issue 4
Publisher: ACM Press
Full text available: pdf(3.09 MB) Additional Information: full citation, references, citings, index terms, review

Results 1 - 20 of 168 Result page: **1** 2 3 4 5 6 7 8 9 next

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player

PORTAL

USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

encrypt$3 and block$3 and "initalization vector"

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used **encrypt$3** and **block$3** and **initalization vector**

Found **2** of **166,357**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 2 of 2

Relevance scale

1 A secure multicast protocol with copyright protection

Hao-hua Chu, Lintian Qiao, Klara Nahrstedt, Hua Wang, Ritesh Jain

April 2002 **ACM SIGCOMM Computer Communication Review**, Volume 32 Issue 2

Publisher: ACM Press

Full text available: pdf(301.97 KB) Additional Information: full citation, abstract, references, citings, index terms

We present a simple, efficient, and secure multicast protocol with copyright protection in an open and insecure network environment. There is a wide variety of multimedia applications that can benefit from using our secure multicast protocol, e.g., the commercial pay-per-view video multicast, or highly secure military intelligence video conference. Our secure multicast protocol is designed to achieve the following goals. (1) It can run in any open network environment. It does not rely on any sec ...

Keywords: copyright protection, key distribution, multicast security, watermark

2 Security Mechanisms in High-Level Network Protocols

Victor L. Voydock, Stephen T. Kent

June 1983 **ACM Computing Surveys (CSUR)**, Volume 15 Issue 2

Publisher: ACM Press

Full text available: pdf(3.23 MB) Additional Information: full citation, references, citings

Results 1 - 2 of 2

Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player

IEEE Xplore® RELEASE 2.1

Home | Login | Logout | Access Information | Alerts |

Welcome United States Patent and Trademark Office

Search Results

BROWSE SEARCH IEEE XPLORE GUIDE

Results for **"(((iv<in>metadata))<and>(encryption<in>metadata))"**

e-mail

Your search matched **9** of **3210** documents.

A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

» Search Options

View Session History

New Search

Modify Search

(((iv<in>metadata))<and>(encryption<in>metadata))

□ Check to search only within this results set

Display Format: ○ Citation ● Citation & Abstract

» Key

IEEE JNL	IEEE Journal or Magazine
IEE JNL	IEE Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IEE CNF	IEE Conference Proceeding
IEEE STD	IEEE Standard

Select Article Information

□ 1. **Generalized eigenvectors and fractionalization of offset DFTs and DCTs**
Soo-Chang Pei; Jian-Jiun Ding;
Signal Processing, IEEE Transactions on [see also Acoustics, Speech, and Sig
IEEE Transactions on]
Volume 52, Issue 7, July 2004 Page(s):2032 - 2046
Digital Object Identifier 10.1109/TSP.2004.828904
Summary: The offset discrete Fourier transform (DFT) is a discrete transform
j2/spl pi/(m-a)(n-b)/N]. It is more generalized and flexible than the original DFT
close relations with the discrete cosine transform (DCT) of type 4 (D.....
AbstractPlus | References | Full Text: PDF(448 KB) IEEE JNL

□ 2. **SCAN-based compression-encryption-hiding for video on demand**
Bourbakis, N.; Dollas, A.;
Multimedia, IEEE
Volume 10, Issue 3, July-Sept. 2003 Page(s):79 - 87
Digital Object Identifier 10.1109/MMUL.2003.1218259
Summary: We present a SCAN-based method for image and video compressi
hiding with application to digital video on demand. The software SCAN implem
on a Pentium IV takes about 1 second for 25 video frames. As an alternative s
AbstractPlus | References | Full Text: PDF(586 KB) IEEE JNL

□ 3. **A multikey secure multimedia proxy using asymmetric reversible parame
theory, design, and implementation**
Yeung, S.F.; Lui, J.C.S.; Yau, D.K.Y.;
Multimedia, IEEE Transactions on
Volume 7, Issue 2, Apr 2005 Page(s):330 - 338
Digital Object Identifier 10.1109/TMM.2005.843361
Summary: Because of limited server and network capacities for streaming app
multimedia proxies are commonly used to cache multimedia objects such that,
nearby proxies, clients can enjoy a smaller start-up latency and receive a bette
AbstractPlus | References | Full Text: PDF(896 KB) IEEE JNL

□ 4. **Generic architecture and semiconductor intellectual property cores for a
encryption standard cryptography**
McLoone, M.; McCanny, J.V.;
Computers and Digital Techniques, IEE Proceedings-
Volume 150, Issue 4, 18 July 2003 Page(s):239 - 244
Digital Object Identifier 10.1049/ip-cdt:20030499
Summary: A generic architecture for implementing the advanced encryption s

encryption algorithm in silicon is proposed. This allows the instantiation of a wi
specifications, with these taking the form of semiconductor intellectual.....

AbstractPlus | Full Text: PDF(490 KB) IEE JNL

□ 5. **A novel image encryption scheme based-on JPEG encoding**
Shiguo Lian; Jinsheng Sun; Zhiquan Wang;
Information Visualisation, 2004. IV 2004. Proceedings. Eighth International Co
14-16 July 2004 Page(s):217 - 220
Digital Object Identifier 10.1109/IV.2004.1320147
Summary: Image encryption is a suitable method to protect image data. The e
algorithms based on position confusion and pixel substitution change compres
In this paper, an image encryption algorithm combining with JPEG encoding is

AbstractPlus | Full Text: PDF(301 KB) IEEE CNF

□ 6. **An IND-CPA cryptosystem from Demytko's primitive**
Galindo, D.; Martin, S.; Morillo, P.; Villar, J.L.;
Information Theory Workshop, 2003. Proceedings. 2003 IEEE
31 March-4 April 2003 Page(s):167 - 170
Summary: An encryption scheme should satisfy semantic security or indisting
encryptions against chosen plaintext attack (IND-CPA). We propose an elliptic
over the ring /spl Zopf/(n/sup 2/), which is efficient and semantically secure.....

AbstractPlus | Full Text: PDF(439 KB) IEEE CNF

□ 7. **A multipath ad hoc routing approach to combat wireless link insecurity**
Lee, C.K.-L.; Xiao-Hui Lin; Yu-Kwong Kwok;
Communications, 2003. ICC '03. IEEE International Conference on
Volume 1, 11-15 May 2003 Page(s):448 - 452 vol.1
Digital Object Identifier 10.1109/ICC.2003.1204217
Summary: As wireless LAN (WLAN) technologies proliferate, it is becoming cc
hoc networks, in which mobile devices communicate via temporary links, are b
products. In the IEEE 802.11b standard, the wired equivalent privacy (WEP) sc

AbstractPlus | Full Text: PDF(435 KB) IEEE CNF

□ 8. **IPSec overhead in wireline and wireless networks for Web and email appl**
Hadjichristofi, G.C.; Davis, N.J., IV; Midkiff, S.F.;
Performance, Computing, and Communications Conference, 2003. Conference
the 2003 IEEE International
9-11 April 2003 Page(s):543 - 547
Summary: This paper focuses on characterizing the overhead of IP security (I
and Web applications using a set of test bed configurations. The different confi
implemented using both wireline and wireless network links. The testing c.....

AbstractPlus | Full Text: PDF(527 KB) IEEE CNF

□ 9. **On belief evolution in authentication protocols**
Kailar, R.; Gligor, V.D.;
Computer Security Foundations Workshop IV, 1991. Proceedings
18-20 June 1991 Page(s):103 - 116
Digital Object Identifier 10.1109/CSFW.1991.151576
Summary: Authentication protocols can be viewed from the perspective of the
beliefs within a protocol run. Inference rules which ensue from this perspective
These rules can be used to analyze the protocols which BAN logic can analy...

AbstractPlus | Full Text: PDF(960 KB) IEEE CNF

Help Contact Us Privacy &

Indexed by
Inspec